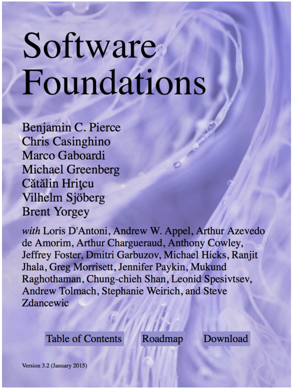
AAA501: Programing Langauge Theory

Lecture 11 — Hoare Logic

Hakjoo Oh
2016 Spring

Acknowledgement

These slides are based on the Hoare Logic chapter of Software Foundations by Pierce et al.



Program Verification

- Using the precise definition of programming languages to formally prove that programs satisfy specifications of their behavior.
- Hoare Logic is a program logic that can be used to reason compositionally about the correctness of programs. Based on two ideas:
  - A natural way of writing down *specifications* of programs.
  - A *compositional proof technique* for proving that programs are correct with respect to the specifications.

Assertions

- Properties that hold at particular points during a program's execution.
- Claims about the current state of the memory when program execution reaches that point. Formally, predicates on memory states, i.e., Memory $\rightarrow$ Bool.
- A set of memory states in which the predicate holds.
- Examples:
  - $\boldsymbol{\lambda s.\ s(x) = 3.}$
  - $\boldsymbol{\lambda s.\ s(x) \leq s(y).}$
  - $\boldsymbol{\lambda s.\ s(x) = 3 \vee s(x) \leq s(y).}$
  - $\boldsymbol{\lambda s.\ s(z) \cdot s(z) \leq s(x)\ \wedge\ \neg((s(z)+1) \cdot (s(z)+1) \leq s(x))}$
  - $\boldsymbol{\lambda s.\ true}$
  - $\boldsymbol{\lambda s.\ false}$

Hoare Triples

- Claims about the behavior of commands.
- $\{P\}\ c\ \{Q\}$
  - "If command c is started in a state satisfying assertion P, and if c eventually terminates in some final state, then this final state will satisfy the assertion Q."
- Formally,

$$\{P\}\ c\ \{Q\} \iff \forall s, s'.\ (c, s) \Downarrow s' \rightarrow P(s) \rightarrow Q(s).$$

Examples

Paraphrase the following Hoare triples in English:

- $\{true\}\ c\ \{x = 5\}$
- $\{x = m\}\ c\ \{x = m + 5\}$
- $\{x \leq y\}\ c\ \{y \leq x\}$
- $\{true\}\ c\ \{false\}$
- $\{x = m\}\ c\ \{y = m!\}$
- $\{true\}\ c\ \{z \cdot z \leq m \wedge \neg((z + 1) \cdot (z + 1) \leq m)\}$

Examples

Which of the following Hoare triples are valid?

- $\{true\}\ x := 5\ \{x = 5\}$
- $\{x = 2\}\ x := x + 1\ \{x = 3\}$
- $\{true\}\ x := 5; y := 0\ \{x = 5\}$
- $\{x = 2 \wedge x = 3\}\ x := 5\ \{x = 0\}$
- $\{true\}\ skip\ \{false\}$
- $\{false\}\ skip\ \{true\}$
- $\{true\}\ while\ true\ do\ skip\ \{false\}$
- $\{x = 0\}\ while\ x == 0\ do\ x := x + 1\ \{x = 1\}$
- $\{x = 1\}\ while\ x \neq 0\ do\ x := x + 1\ \{x = 100\}$

Two Simple Facts

1. $\forall P, Q, c.\ (\forall s.\ Q(s)) \rightarrow \{P\}\ c\ \{Q\}.$
2. $\forall P, Q, c.\ (\forall s.\ \neg P(s)) \rightarrow \{P\}\ c\ \{Q\}.$

Proof Rules of Hoare Logic

- Hoare logic provides a set of proof rules for compositionally proving the validity of Hoare triples.
  - The structure of a program's correctness mirrors the structure of the program.
  - One rule for reasoning about each of the different syntactic forms of commands, plus structural rules that are used for gluing things together.

- Hoare triples are proved using the proof rules, without relying on the definition of Hoare triples.

Assignment

$$\{Q[x \mapsto e]\}\ x := e\ \{Q\}$$

- $\{y = 1\}\ x := y\ \{x = 1\}$
- $\{?\}\ x := y + z\ \{x = 1\}$
- $\{?\}\ x := x + 1\ \{x \leq 5\}$
- $\{?\}\ x := 3\ \{x = 3\}$
- $\{?\}\ x := 3\ \{0 \leq x \wedge x \leq 5\}$

Skip and Sequence

$$\{P\}\ skip\ \{Q\}$$

$$\frac{\{P\}\ c_1\ \{Q\} \quad \{Q\}\ c_2\ \{R\}}{\{P\}\ c_1; c_2\ \{R\}}$$

Consequence

$$\frac{P \rightarrow P' \qquad \{P'\}\ c\ \{Q'\} \qquad Q' \rightarrow Q}{\{P\}\ c\ \{Q\}}$$

Conditional

$$\frac{\{P \wedge b\}\ c_1\ \{Q\} \qquad \{P \wedge \neg b\}\ c_2\ \{Q\}}{\{P\}\ \mathit{if}\ b\ c_1\ c_2\ \{Q\}}$$

Loops

$$\frac{\{P \wedge b\}\ c\ \{P\}}{\{P\}\ while\ b\ c\ \{P \wedge \neg b\}}$$

Exercise

$$\{x \leq 3\}\ while\ x \leq 2\ do\ x := x + 1\ \{x = 3\}$$

Hoare Logic

Idea: a *domain specific logic* for reasoning about properties of programs

- This hides the low-level details of the semantics of the program
- Leads to a compositional reasoning process

$$\{Q[x \mapsto e]\}\ x := e\ \{Q\}$$

$$\{P\}\ skip\ \{Q\}$$

$$\frac{\{P\}\ c_1\ \{Q\} \quad \{Q\}\ c_2\ \{R\}}{\{P\}\ c_1; c_2\ \{R\}}$$

$$\frac{P \to P' \qquad \{P'\}\ c\ \{Q'\} \qquad Q' \to Q}{\{P\}\ c\ \{Q\}}$$

$$\frac{\{P \land b\}\ c_1\ \{Q\} \qquad \{P \land \neg b\}\ c_2\ \{Q\}}{\{P\}\ if\ b\ c_1\ c_2\ \{Q\}}$$

$$\frac{\{P \land b\}\ c\ \{P\}}{\{P\}\ while\ b\ c\ \{P \land \neg b\}}$$